

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»**

ЗАТВЕРДЖУЮ:

Президент

Національного університету

«Києво-Могилянська академія»

Сергій КВІТ

(підпис)

_____ 20 ____ р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНИХ СИСТЕМ»

(«Information systems vulnerability analysis»)

першого (бакалаврського) рівня вищої освіти

за спеціальністю F5 Кібербезпека та захист інформації

галузі знань F Інформаційні технології

Кваліфікація: бакалавр з кібербезпеки та захисту інформації

ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ ЗАТВЕРДЖЕНО

Вченою радою НаУКМА

Протокол № 7 від 27 квітня 2023 р.

ЗМІНИ ДО ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗАТВЕРДЖЕНО

Вченою радою НаУКМА

Голова вченої ради НаУКМА

І. Г. Лук'яненко _____

(Протокол № ____ від _____ 2025 р.)

Київ – 2026

ЛИСТ ПОГОДЖЕННЯ
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«Аналіз вразливостей інформаційних систем»
(«Information systems vulnerability analysis»)

Віцепрезидент з науково-педагогічної
роботи

(підпис)

Зоряна ЛУЦИШИН

Начальник навчально-методичного
відділу

(підпис)

Ірина РУДЬ

Робоча група:

Керівник робочої групи/гарант ОП:

(підпис)

Тетяна САВЧЕНКО

Члени групи:

(підпис)

Андрій ГЛИБОВЕЦЬ

(підпис)

Микола ГЛИБОВЕЦЬ

(підпис)

Семен ГОРОХОВСЬКИЙ

(підпис)

Олександр ЖЕЖЕРУН

(підпис)

Трохим БАБИЧ

(підпис)

Катерина ЗВІРКОВА

ПЕРЕДМОВА

Розроблено робочою групою у складі:

1. *Савченко Тетяна Віталіївна* – кандидат технічних наук, доцент кафедри інформатики, керівник робочої групи / гарант освітньої програми;
2. *Глибовець Андрій Миколайович* – доктор технічних наук, декан факультету інформатики, професор кафедри мережних технологій;
3. *Глибовець Микола Миколайович* – доктор фізико-математичних наук, професор кафедри інформатики, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки;
4. *Гороховський Семен Самуїлович* – кандидат фізико-математичних наук, доцент, завідувач кафедри інформатики;
5. *Олецький Олексій Віталійович* – доцент кафедри мультимедійних систем, кандидат технічних наук;
6. *Жежерун Олександр Петрович* – завідувач кафедри мультимедійних систем, кандидат фізико-математичних наук, доцент, керівник робочої групи;
7. *Бабич Трохим Анатолійович* – заступник декана факультету інформатики, старший викладач кафедри інформатики;
8. *Звірко Катерина Олегівна* – студентка факультету інформатики, 3 курсу, спеціальності «Кібербезпека та захист інформації».

Рецензії / відгуки стейкхолдерів:

- Олександр Потій – доктор технічних наук, професор, бригадний генерал, заступник Голови Держспецзв’язку;
- Назар Тимошик – кандидат технічних наук, власник групи компаній з кібербезпеки «UnderDefense»;
- Степан Веселовський – виконавчий директор Львівського ІТ Кластеру;
- Роман Сологуб – генеральний директор ТОВ «ІССП Сервіс»;
- Єгор Аушев – директор CyberUnit.

1. ПРОФІЛЬ ОСВІТНЬОЇ ПРОГРАМИ

F5 «Кібербезпека та захист інформації»

1 – Загальна інформація	
Повна назва закладу вищої освіти та структурного підрозділу	Національний університет «Києво-Могилянська академія» Факультет інформатики Кафедра інформатики
Рівень вищої освіти	Перший (бакалаврський) рівень
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Ступінь вищої освіти – бакалавр Освітня кваліфікація: бакалавр з кібербезпеки та захисту інформації
Офіційна назва освітньої програми	Аналіз вразливостей інформаційних систем / Information systems vulnerability analysis
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 3 роки 10 місяців, 240 кредитів ЄКТС
Тип програми	Освітньо-професійна Educational professional
Наявність акредитації	Акредитація відсутня
Передумови	Наявність атестату про повну загальну середню освіту
Цикл/рівень програми	НРК України – 6 рівень, FQ-EHEA – перший цикл, EQF-LLL – 6 рівень
Мова (и) викладання	Українська
Форма навчання	Денна
Термін дії освітньої програми	Відповідно до терміну акредитації
Інтернет адреса постійного розміщення опису освітньо-професійної програми	https://www.fin.ukma.edu.ua
2 – Мета освітньої програми	
Мета програми (з врахуванням рівня кваліфікації)	Підготовка фахівців з кібербезпеки та захисту інформації, здатних проводити теоретичні та практичні дослідження в галузі аналізу та оцінки вразливостей інформаційних технологій; застосовувати математичні методи та алгоритмічні принципи в оцінці ризиків та моделюванні потенційних загроз; здійснювати розробку та впровадження заходів зі зниження вразливості інформаційних систем; аналізувати технічні та організаційні аспекти кібербезпеки, розробляти та оцінювати ефективність заходів кібербезпеки в інформаційних системах.
3 - Характеристика освітньої програми	
Предметна область (галузь знань / спеціальність)	Галузь знань – F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації

	Об'єкти вивчення: – технології кібербезпеки та захисту інформації; – процеси управління кібербезпекою та захистом інформації; об'єкти інформаційної діяльності, в тому числі інформаційні та інформаційно-комунікаційні системи, інформаційні ресурси і технології. Цілі навчання: підготовка фахівців, здатних використовувати і впроваджувати технології кібербезпеки та захисту інформації та розв'язувати складні задачі у галузі кібербезпеки та захисту інформації. Теоретичний зміст предметної області: Принципи, концепції, теорії захисту життєво важливих інтересів людини, суспільства, держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Методи, методики та технології: методи, методики та технології розв'язання теоретичних і практичних задач кібербезпеки та захисту інформації. Інструменти та обладнання: засоби, пристрої, мережне устаткування, прикладне та спеціалізоване програмне забезпечення, інформаційні системи та комплекси проектування, моделювання, контролю, моніторингу, зберігання, обробки, відображення та захисту даних (інформаційних потоків).
Орієнтація освітньої програми	Освітньо-професійна програма з кібербезпеки та захисту інформації орієнтована на підготовку фахівців, що поєднують фундаментальні математичні, аналітичні, інформаційні та правові положення з практичними навичками роботи у сфері кібербезпеки та захисту інформації, пошуком та експлуатацією вразливостей в інформаційних системах на всіх рівнях: програмному забезпеченні, веб-сайтах, корпоративних мережах.
Основний фокус освітньої програми та спеціалізації	Спеціальна освіта за спеціальністю F5 «Кібербезпека та захист інформації». Програма спрямована на вивчення вразливостей інформаційних систем та мереж; методів і технологій виявлення та аналізу вразливостей; математичних, інформаційних та імітаційних моделей для аналізу вразливостей інформаційних систем та мереж; методів та технологій кібербезпеки інформаційних систем та мереж;

	методів і технологій зберігання, обробки, передачі та захисту інформації. Акцент програми здійснено на поглиблення теоретичних та практичних знань в галузі кібербезпеки та інформаційних технологій, зокрема, формування навичок оцінки вразливостей і практичної реалізації заходів щодо їх запобігання. Ключові слова: науки про кібербезпеку, оцінка вразливостей, аналіз даних, виявлення та виправлення вразливостей, безпека програмного забезпечення.
Особливості програми	Освітня програма має прикладний, практико-орієнтований характер і спрямована на підготовку фахівців, здатних здійснювати повний цикл робіт з виявлення, аналізу, оцінки та усунення вразливостей в інформаційних системах і мережах, а також проводити аудит безпеки відповідно до національних і міжнародних стандартів. Особливість програми полягає у формуванні не лише технічних знань, а й у розгляді питань, пов'язаних з етичними та правовими нормами, розвитку аналітичного та управлінського мислення, необхідного для роботи у командах кіберзахисту.
Базова загальновійськова підготовка громадян України, які здобувають вищу освіту	Програма призначена для підготовки громадян, які здобувають вищу освіту, спрямована на формування знань, умінь і навичок, необхідних для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть бути працевлаштовані на посади у структурних підрозділах установ / підприємств / організацій, які передбачають наявність вищої освіти зі спеціальності F5 Кібербезпека та захист інформації (першого бакалаврського рівня вищої освіти). Фахівець спроможний виконувати професійні роботи і займати посади, визначені Національним класифікатором України «Класифікатор професій ДК 003:2010», зокрема: 2139.2 Фахівець з реагування на інциденти та 4113 Кібероператор. Випускник може обіймати й інші посади відповідно до професійних назв робіт, що характеризуються спеціальними (фаховими) компетентностями.
Подальше навчання	Можливості продовження освіти за другим (магістерським) рівнем вищої освіти. Набуття

		додаткових кваліфікацій в системі післядипломної освіти
5 – Викладання та оцінювання		
Викладання та навчання		Підходами до навчання є: компетентнісний, студентоцентризований та проблемно-орієнтований. Провідні методи навчання – проблемний, частково-пошуковий та дослідницький. Викладання та навчання проводиться у форматі лекцій, серед яких, інтерактивні та мультимедійні, практичні заняття, лабораторні роботи, самостійне навчання, курсове дослідження.
Оцінювання		Оцінювання навчальних досягнень здійснюється відповідно до «Положення про організацію освітнього процесу в Національному університеті «Києво-Могилянська академія»», «Положення про критерії оцінювання знань здобувачів вищої освіти в Національному університеті «Києво-Могилянська академія»», Положення про рейтингову систему оцінювання знань і компетентностей здобувачів вищої освіти Національного університету «Києво-Могилянська академія» за 100-бальною шкалою. Письмові та усні іспити, звіти до лабораторних та практичних робіт, усні презентації, поточний контроль, заліки, захист кваліфікаційної роботи бакалавра. ЄДКІ передбачає оцінювання досягнень результатів навчання, визначених Стандартом вищої освіти за спеціальністю 125 Кібербезпека та захист інформації за даною освітньою програмою.
6 – Програмні компетентності		
Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	
Загальні компетентності (ЗК)	ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК4. Здатність спілкуватися іноземною мовою. ЗК5. Здатність вчитися і оволодівати сучасними знаннями. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення й діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності. ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній	

	системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ЗК9. Здатність захищати Батьківщину.
Спеціальні (фахові, предметні) компетентності (СК)	СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності. СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації. СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації. СК5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо). СК7. Здатність здійснювати професійну діяльність на основі впровадженної системи управління інформаційною та кібербезпекою. СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності. СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності. СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.
7 – Результати навчання	
Результати навчання (РН)	РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків. РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації. РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недобросовісності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність. РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення. РН6. Адаптуватися до нових умов і технологій професійної діяльності,

прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11. Планувати підготовку та забезпечувати неперервність бізнес-процесів і організацій згідно зі встановленою політикою кібербезпеки з урахуванням вимог до захисту інформації.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і

	заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації. РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах. РН22. Мати додаткові знання, уміння та навички необхідні для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	До реалізації освітньої програми залучаються науково-педагогічні працівники, що відповідають ліцензійним вимогам, мають науковий ступінь та/або вчене звання за відповідною або спорідненою спеціальністю, їх базова освіта відповідає профілю освітніх компонент, які вони викладають, а також висококваліфіковані спеціалісти та фахівці-практики.
Матеріально-технічне забезпечення	Забезпеченість приміщеннями для проведення навчальних занять та контрольних заходів. Забезпеченість мультимедійним обладнанням для одночасного використання в навчальних аудиторіях. Наявність соціально-побутової інфраструктури. Забезпечення здобувачів вищої освіти гуртожитком. Забезпечення комп'ютерними робочими місцями, лабораторіями, полігонами, обладнанням, устаткуванням необхідними для виконання навчальних планів.
Інформаційне та навчально-методичне забезпечення	Використання платформи електронного навчання факультету інформатики (https://distedu.ukma.edu.ua/) та авторських розробок науково-педагогічних працівників факультету. Забезпеченість бібліотеки вітчизняними та закордонними фаховими періодичними виданнями відповідного або спорідненого профілю. Наявність доступу до баз даних періодичних наукових видань англійською мовою відповідного або спорідненого профілю. Наявність офіційного веб-сайту Національного університету «Києво-Могилянська академія» на якому розміщена основна інформація про його діяльність (структура, ліцензії та сертифікати про акредитацію, освітня/освітньо-професійна/видавнича/атестаційна (наукових кадрів) діяльність, навчальні та наукові структурні підрозділи та їх склад, перелік навчальних дисциплін, правила прийому, контактна інформація). Наявність електронного ресурсу закладу освіти, який містить навчально-методичні матеріали з дисциплін навчального плану в тому числі в системі дистанційного навчання. Необмежений доступ до мережі Інтернет, друковані та Інтернет-джерела (у т.ч. Центр електронного навчання Національного університету «Києво-Могилянська академія») інформації; навчальні і робочі плани (з пояснювальними записками до них), освітні програми, робочі програми дисциплін і практик, навчально-методичні комплекси дисциплін, що включають лекційний матеріал, завдання практичних робіт, питання семінарських занять, завдання самостійної роботи, питання, задачі, завдання для поточного та підсумкового контролю. Відповідає ліцензійним умовам – 100%.

9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти України. Можлива, за бажанням студента.
Міжнародна кредитна мобільність	На основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти зарубіжних країн партнерів. Можлива, за бажанням студента
Навчання іноземних здобувачів вищої освіти	Навчання іноземних студентів проводиться на загальних умовах на основі двосторонніх договорів (угод) між Національним університетом «Києво-Могилянська академія» та закладами вищої освіти іноземних країн. Громадяни інших держав приймаються на навчання на підставі міжнародних договорів на умовах, визначених цими договорами, а також договорів, укладених навчальним закладом із зарубіжними навчальними закладами, організаціями, або індивідуальних договорів, контрактів.

2. ПЕРЕЛІК КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1. Перелік освітніх компонентів освітньо-професійної програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота)	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові освітні компоненти ОП			
1.1. Навчальні дисципліни			
ОК 1.	Адміністрування розподілених систем	4,00	екзамен
ОК 2.	Алгоритми і структури даних	6,00	екзамен
ОК 3.	Англійська мова	7,00	екзамен
ОК 4.	Англійська мова (за професійним спрямуванням)	7,00	екзамен
ОК 5.	Архітектура обчислювальних систем	4,00	екзамен
ОК 6.	Бази даних	4,00	екзамен
ОК 7.	Безпека веб-застосунків	4,00	екзамен
ОК 8.	Безпека операційних систем	4,00	екзамен
ОК 9.	Безпека програмних впроваджень	4,00	екзамен
ОК 10.	Веб-програмування	4,00	екзамен
ОК 11.	Диференціальні рівняння	3,00	екзамен
ОК 12.	Етичний хакінг	4,00	екзамен
ОК 13.	Етичні аспекти кібербезпеки	2,00	екзамен
ОК 14.	Інфраструктура безпеки організацій	4,00	екзамен
ОК 15.	Історія української кібернетики	2,00	екзамен
ОК 16.	Криптографія	4,00	екзамен
ОК 17.	Курсова робота	3,00	екзамен
ОК 18.	Лінійна алгебра та аналітична геометрія	4,00	екзамен
ОК 19.	Методи та засоби соціальної інженерії	2,00	екзамен
ОК 20.	Мова програмування Python	6,00	екзамен
ОК 21.	Моделі обчислень в програмній інженерії	4,00	екзамен
ОК 22.	Низькорівневі вразливості програмного забезпечення	2,00	екзамен
ОК 23.	Організація та управління командною роботою	4,00	екзамен
ОК 24.	Основи веб-технологій	3,00	екзамен
ОК 25.	Основи дискретної математики	4,00	екзамен
ОК 26.	Методи захисту у кібербезпеці	4,00	екзамен
ОК 27.	Основи матаналізу	4,00	екзамен
ОК 28.	Основи мережевої безпеки	3,00	екзамен
ОК 29.	Основи мережних технологій	5,00	екзамен
ОК 30.	Основи операційних систем	4,00	екзамен
ОК 31.	Правове регулювання в галузі кібербезпеки	4,00	екзамен
ОК 32.	Процедурне програмування	5,00	екзамен
ОК 33.	Розробка та впровадження програмних продуктів	4,00	екзамен
ОК 34.	Теорія алгоритмів і математична логіка	4,00	екзамен
ОК 35.	Теорія ймовірностей та математична статистика	4,00	екзамен
ОК 36.	Українська мова за професійним спрямуванням	5,00	екзамен
ОК 37.	Хмарні технології	4,00	екзамен

<i>1.2. Практика</i>			
ОК 38.	Практика виробнича	3,00	залік
ОК 39.	Практика навчальна	3,00	залік
2. Вибіркові освітні компоненти ОП*			
<i>2.1. Навчальні дисципліни професійної підготовки</i>			
ВК 1.	Електроніка та цифрова електроніка	3,0	залік
ВК 2.	Мережна маршрутизація	3,0	залік
ВК 3.	Локальні мережі	3,0	залік
ВК 4.	Розробка клієнт серверних застосувань	3,0	залік
ВК 5.	Front-end та Back-end - технології веб-застосувань	4,0	залік
ВК 6.	Основи роботи з фреймворком Spring Boot	5,5	залік
ВК 7.	Схемотехніка	3,5	залік
ВК 8.	Мова програмування Swift	3,0	залік
ВК 9.	Хмарні технології	4,0	залік
ВК 10.	Методи та засоби збору чутливої інформації	2,0	залік
ВК 11.	Вступ до мікросервісної архітектури з використанням Spring Boot	4,0	залік
ВК 12.	Технології сучасних дата – центрів	4,0	залік
ВК 13.	Адміністрування Unix-систем	3,0	залік
ВК 14.	Розробка та експлуатація банківських комп'ютерних систем	4,5	залік
ВК 15.	Прикладне програмування мобільних систем на основі ОС Android	4,0	залік
ВК 16.	Технологія веб-програмування Ruby on Rails	4,0	залік
ВК 17.	Основи технології блокчейн і криптовалюти	4,0	залік
ВК 18.	Основи фреймворку скрам	3,0	залік
ВК 19.	Робота з неструктурованими даними	4,0	залік
ВК 20.	Програмування мікроконтролерів та операційні системи реального часу	5,0	залік
ВК 21.	Математичні методи обробки зображень	4,0	залік
ВК 22.	Обчислювальне суспільствознавство	2,5	залік
ВК 23.	Інформаційний пошук	4,0	залік
ВК 24.	Обробка зображень та мультимедіа	4,0	залік
ВК 25.	Автоматизація роботи з програмними проектами мовою Java	3,0	залік
ВК 26.	Дані та суспільство	3,5	залік
ВК 27.	Математичні методи дослідження операцій	4,0	залік
ВК 28.	Методи об'єктно-орієнтованого програмування	4,0	залік
ВК 29.	Обчислювальна геометрія	4,5	залік
ВК 30.	Спецкурс з комп'ютерної алгебри	4,0	залік
ВК 31.	Технології мультимедіа	3,0	залік
ВК 32.	Інтернет речей (Internet of Things)	4,0	залік
ВК 33.	Методи та засоби обробки інформації	3,0	залік
ВК 34.	Основи комп'ютерної алгебри	4,0	залік
ВК 35.	Практичні основи роботи з базами даних в Spring Boot	3,0	залік
ВК 36.	Розробка iOS додатків	4,0	залік
ВК 37.	Теорія складності обчислень	4,0	залік

2.2. Навчальні дисципліни вільного вибору			
ВБ 1.	Вступ до ігрової розробки	4,0	залік
ВБ 2.	Теорія чисел	4,5	залік
ВБ 3.	Основи фотографії	2,5	залік
ВБ 4.	Англійська мова – 2	7,0	іспит
ВБ 5.	Розробка користувацького інтерфейсу (UI/UX)	4,5	залік
ВБ 6.	Дизайн веб-інтерфейсів	3,0	залік
ВБ 7.	Базова загальноїсськова підготовка громадян України, які здобувають вищу освіту (теоретична підготовка) ***	3,0	залік
ВБ 8.	Базова загальноїсськова підготовка громадян України, які здобувають вищу освіту (практична підготовка) ****	7,0	залік
3. Атестація			
ОК 40.	Підготовка до ЄДКІ	-	-
ОК 41.	Кваліфікаційна робота	15,0	теза
Загальний обсяг обов'язкових компонент:		173	
Обсяг вибірових освітніх компонентів ОП (за зведеними даними навчального плану)		67	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНОЇ ПРОГРАМИ		240	

ВК Перелік компонент ОП

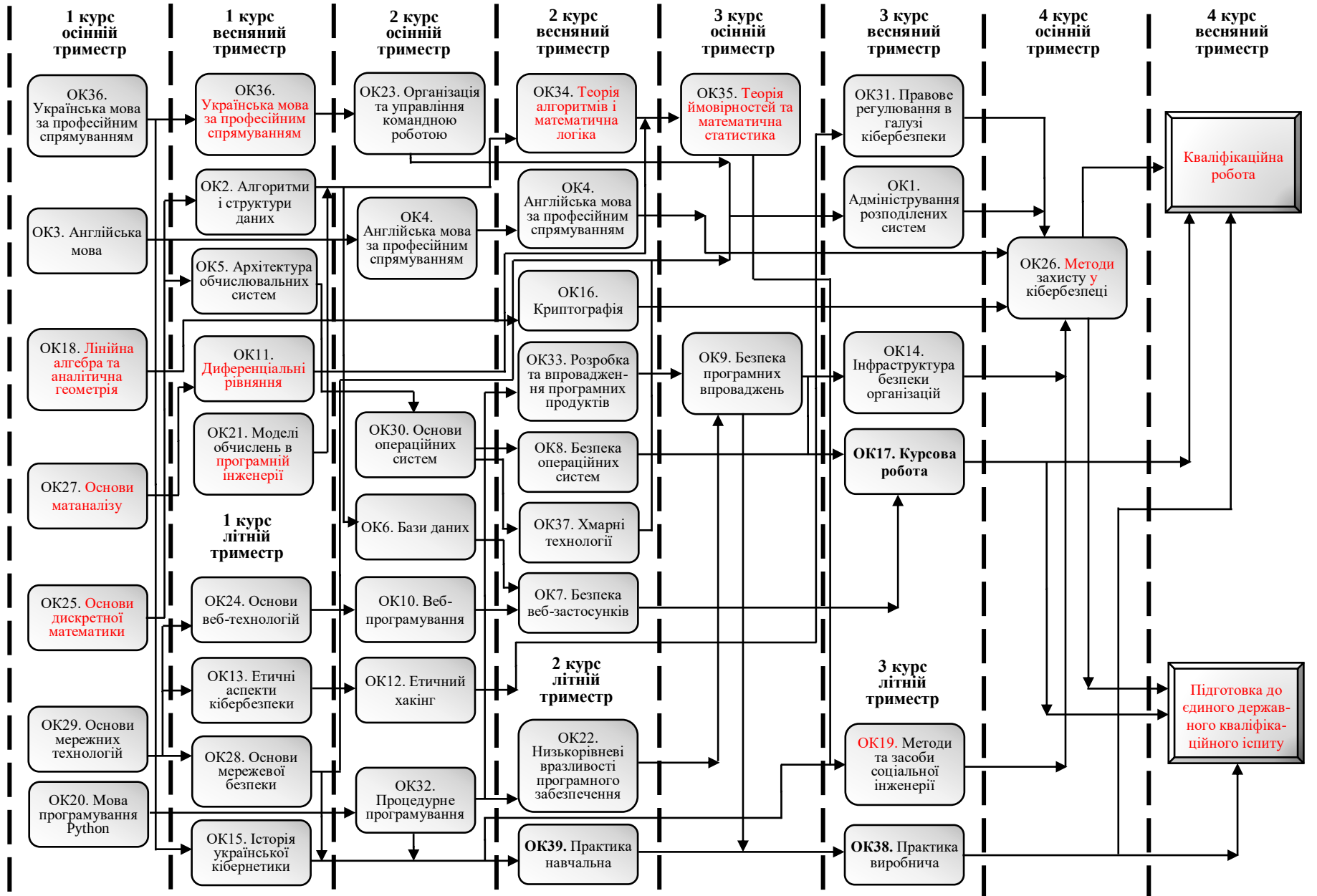
* Згідно з п.п. 2.2.2-2.2.7 «Положення про порядок реалізації студентами Національного університету «Києво-Могилянська академія» права на вільний вибір дисциплін» здобувачі освіти мають безумовне право обрати навчальні дисципліни з обов'язкових та вибірових частин навчальних планів інших спеціальностей того самого рівня, а за умови погодження із деканом факультету – з програм іншого рівня.

** Перелік навчальних дисциплін для вибірової складової та робочі програми навчальних дисциплін представлено на офіційному сайті університету: <https://my.ukma.edu.ua>

*** Обов'язкова дисципліна для здобувачів вищої освіти 2-го року навчання чоловічої статі. Для інших здобувачів – вибірова.

**** Обов'язкова дисципліна для здобувачів вищої освіти 2-го року навчання чоловічої статі, які пройшли теоретичну підготовку з освітнього компонента. Для інших здобувачів – вибірова.

2.2. Структурно-логічна схема освітньо-професійної програми



3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Атестація здобувачів вищої освіти зі спеціальності F5 «Кібербезпека та захист інформації» здійснюється у формі єдиного державного кваліфікаційного іспиту та публічного захисту кваліфікаційної роботи.

Кваліфікаційна робота має передбачати розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації. У кваліфікаційній роботі не має бути академічного плагіату, фальсифікації та фабрикації. Кваліфікаційна робота має бути оприлюднена (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті університету або факультету, або на платформі електронного навчання DistEdu.

Атестація здійснюється Екзаменаційною комісією, яка затверджується наказом президента Національного університету «Києво-Могилянська академія». Екзаменаційна комісія приймає рішення про присвоєння студенту-випускнику кваліфікації бакалавра з кібербезпеки та захисту інформації та видає диплом державного зразка.

Цей диплом є юридичним документом, який дозволяє фахівцю займати первинні посади у відповідності з їх переліком та діючою в Україні відповідною номенклатурою посад.

Атестація здійснюється відкрито і публічно.

До єдиного державного кваліфікаційного іспиту та захисту кваліфікаційної роботи бакалавра допускаються студенти, які виконали всі вимоги навчального плану. Атестація має своєю метою з'ясування рівня підготовленості випускника для виконання професійних завдань, передбачених відповідними стандартами вищої освіти, і продовження освіти.

Публічний захист (демонстрація) кваліфікаційної роботи передбачає: представлення основних положень роботи у вигляді мультимедійної презентації та пояснювальної записки; відкриту форму засідання комісії; оголошення в той же день після закінчення захисту оцінки кваліфікаційної роботи та оформлення протоколу засідання комісії; ухвалення комісією рішення про присвоєння кваліфікації з кібербезпеки та захисту інформації та видачу диплома бакалавра за результатами підсумкової атестації.

4. МАТРИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ ТА СПЕЦІАЛЬНИХ ПРОГРАМНИХ КОМПЕТЕНТНОСТЕЙ КОМПОНЕНТАМ ОСВІТНЬОЇ ПРОГРАМИ

Програмні компетентності	Обов'язкові освітні компоненти (ОК) ОП																																																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	ВБ 7	ВБ 8						
Загальні компетентності																																																	
ЗК1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			
ЗК2	+	+			+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		
ЗК3															+		+						+								+					+		+	+	+	+	+	+	+	+	+			
ЗК4			+	+																+			+								+	+	+																
ЗК5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+		+		+					
ЗК6													+																			+																	
ЗК7	+						+	+	+			+	+	+			+		+			+	+			+		+	+		+						+												
ЗК8													+		+																					+					+		+						
ЗК9							+	+	+			+	+	+	+							+				+		+				+												+	+	+	+	+	
Спеціальні (фахові) компетентності спеціальності																																																	
СК1			+	+									+				+								+						+										+								
СК2	+	+			+	+	+	+	+	+		+				+	+		+	+	+	+	+	+	+		+		+	+	+	+	+	+	+				+	+	+	+	+	+					
СК3	+				+	+	+	+	+	+		+	+	+					+	+		+	+	+		+		+	+	+	+	+	+	+	+				+	+	+	+	+	+					
СК4	+	+			+	+	+	+	+	+		+		+			+		+	+		+	+	+		+		+	+	+		+	+				+	+	+	+	+	+							
СК5	+	+					+	+	+			+		+							+				+		+													+	+								
СК6	+				+	+							+	+											+		+													+	+	+	+						
СК7	+	+			+	+	+	+	+	+		+	+	+		+	+		+	+	+	+	+	+		+		+	+	+	+	+	+	+	+				+	+	+	+	+	+					
СК8	+						+	+	+		+	+				+	+					+				+		+												+	+	+	+	+					
СК9	+				+		+	+	+			+					+					+				+		+												+	+	+	+	+					
СК10	+	+	+	+	+		+		+			+	+	+			+	+	+	+		+			+	+	+	+	+			+	+	+	+			+	+	+	+	+	+	+	+				

5. МАТРИЦЯ ЗАБЕЗПЕЧЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ (РН) КОМПОНЕНТАМИ ОПП

Програмні результати навчання	Обов'язкові освітні компоненти (ОК) ОП																																																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	ВБ 7	ВБ 8						
PH1															+		+					+									+					+		+	+	+	+	+	+						
PH2			+	+																+			+								+	+	+																
PH3	+						+	+	+			+	+	+			+		+			+	+			+		+	+		+						+												
PH4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
PH5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		
PH6	+	+			+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
PH8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+			+		+						
PH9			+	+									+				+										+					+										+							
PH10	+	+			+	+	+	+	+	+		+				+	+		+	+	+	+	+	+		+		+	+	+	+	+	+	+				+	+	+	+	+	+	+	+				
PH11	+				+	+	+	+	+	+		+	+	+					+	+		+	+	+		+		+	+	+	+	+	+	+				+	+	+	+	+	+	+	+				
PH12	+	+			+	+	+	+	+	+		+		+			+		+	+		+	+	+		+		+	+	+		+	+				+	+	+	+	+	+	+	+	+				
PH13	+	+			+	+	+	+	+	+		+		+			+		+	+		+	+	+		+		+	+	+		+	+				+	+	+	+	+	+	+	+	+				
PH14	+	+					+	+	+			+		+								+				+		+												+	+								
PH15	+	+					+	+	+			+		+								+				+		+													+	+							
PH16	+				+	+							+	+												+		+													+	+	+	+					
PH17	+	+			+	+	+	+	+	+		+	+	+		+	+		+	+	+	+	+	+		+		+	+	+	+	+	+	+	+			+	+	+	+	+	+	+	+				
PH18	+						+	+	+		+	+				+	+					+				+		+												+	+	+	+	+					
PH19	+						+	+	+		+	+				+	+					+				+		+													+	+	+	+	+				
PH20	+				+		+	+	+			+					+					+				+		+												+	+	+	+	+					
PH21	+	+	+	+	+		+		+			+	+	+			+	+	+	+		+			+	+	+	+	+			+	+	+	+	+		+	+	+	+	+	+	+	+				
PH22						+	+	+	+			+	+	+															+	+																	+	+	

Гарант освітньої програми: Савченко Тетяна Віталіївна – кандидат технічних наук, доцент кафедри інформатики

_____ «_____» _____ 202__ р.